./ solwall

CYBER SECURITY EXPERTS & SYSTEM INTEGRATORS

DATA SHEET

Offensive Cybersecurity

Can you risk disclosure of your critical intellectual property, personal data or private financial information for a few days or even weeks of downtime?

Benefits

- Know whether your company is safe
- Mitigate threats before attackers exploit them
- Solwall team behave like real hacker
- Manual approach can’t be repeated with automated testing tools

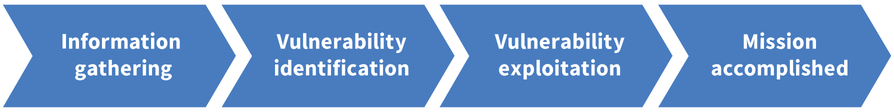
Why Solwall

Our experts follow the latest trends in cybersecurity and have more than 20 years of experience in the field. We deeply understand the ever-evolving techniques and procedures of real hackers. We know what they do and how they do it so that we can prevent it.

Service overview

An enterprise must maintain a robust and attack-resilient infrastructure in order to successfully defend against cyber-attacks. Solwall’s methodology and tools are adapted to suit each client’s environment and objectives. Offensive cybersecurity consists of individual services packaged to provide a costly effective proactive service. Our penetration testing is carefully designed to protect the business from any inadvertent downtime.

Approach



Information gathering

Vulnerability identification

Vulnerability exploitation

Mission accomplished

Understand the system before the real attacks are planned.

Discover the vulnerabilities within the target environment.

Gain access by exploiting identified vulnerabilities with internally developed tools.

Report detailed findings with a mitigation plan and try to move further.

Assessments can be performed without prior knowledge of your system (black-box) or with knowledge about your environment (white-box).

What you get

- An executive summary with strategic recommendations for long-term improvements
- Technical details with a mitigation plan for immediate improvements
- Attack recreate details
- Remediation assistance

Range of offensive cybersecurity services

Service	Objective	Benefit
External security assessment	Identify and evaluate security vulnerabilities of company's infrastructure and recommend risk mitigation strategies	Understand Internet footprint and associated risks to your environment
Internal security assessment	Simulate an attack from an internal network to access end-user systems, including escalation of privileges and access to critical data	Understand how good your internal security is and what might be a risk to your business from a breach
Red teaming	Simulate behavior of a real hacker and try to compromise your environment from the internet	Test attack detection and response capabilities of your security team - without real risk
Mobile application assessment	Recognize and define security threats that can lead to data exposure or unauthorized access	Understand and improve security of your mobile application
Web application assessment	Recognize and define security threats that can lead to data exposure or unauthorized access	Understand and improve security of your web application
Configuration audit	Compare system configuration against best practices defined by global community of security experts	Improving your security by tightening of the operating system rules and software version checks
Social engineering	Determine the credibility and loyalty of the employees towards the company and its security policies	Prepare company and employees against social engineering attacks
Source code review	Examine an application source code to find errors overlooked in initial phase of development	Identifying vulnerabilities at the root level

Would you like to know more? Contact us at info@solwall.com or visit www.solwall.com

Solwall d.o.o.

Ukmarjeva ul. 4
1000 Ljubljana
Slovenia

+1 4156 925 264
info@solwall.com
www.solwall.com

About us

Solwall is helping enterprises protect their valuable data, fight against cyber-attacks and reduce security risk enabling them to have risk-free future. We earn customer trust and loyalty by providing superb value and quality.